REMARKS

In the Office Action, the Examiner has determined that this application does not contain an abstract of the disclosure. Applicant respectfully disagrees with this determination and notes that the original international application included an abstract. Nonetheless, Applicant has attached a substitute abstract hereto.

In the Office Action, claims 1-22 were rejected. More specifically,

- Claims 1-22 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite;
- Claims 1-22 were rejected under 35 U.S.C. § 102(a) as being anticipated by the paper published in the journal "Advances in Applied Mathematics, vol. 16, No.1" (the Mittenthal paper);
- Claims 16 and 18 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,182,216 (Luyster);
- Claims 1-15, 17 and 19-22 were rejected under 35 U.S.C. § 103(a) as being obvious over Luyster; and
- Claims 1-22 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-34 of U.S. Patent 6,035,042 (Mittenthal).

For the reasons set forth hereinbelow, Applicants request that the §§ 112, 102(a), 102(e), 103(a) and obviousness-type double patenting rejections associated with the pending claims be withdrawn.

§ 112 Rejections

Claims 1-22

Applicant respectfully disagrees with the Examiner's determination that claims 1-22 fail to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

First, Applicant respectfully disagrees with the Examiner's determination that the term "maximal" is used in claims 1-22 to mean "a function that can be applied recursively to generate the entire orthomorphic mapping." To the contrary, Applicant notes that the term "maximal nonlinear" in claim 1 and elsewhere, is used as an adjective denoting a quality of the recited block substitution tables.

Second, Applicant submits that nonlinearity is a well-defined mathematical term defining functions or mappings which are not linear.

Third, Applicant submits that nonlinearity is a measurable property and that there is a maximal level of nonlinearity which cannot be exceeded.

Therefore, Applicant submits that independent claims 1-22 are not indefinite for reciting "maximal nonlinear" block substitution tables. Accordingly, Applicant respectfully requests that the § 112 rejections associated with the pending claims be withdrawn.

§ 102(a) Rejections

Claims 1-15

Applicant respectfully submits that independent claim 1 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 1. *See* MPEP § 2131 (stating that a claim is anticipated only if each and every element as set forth in the claim is disclosed in a single prior art reference). More specifically, Applicant submits that the paper fails to disclose, among other things, "creating maximal nonlinear block substitution tables" as recited in independent claim 1.

First, Applicant notes that generating functions of orthomorphisms are special polynomials, not the one-half of a block of binary bits disclosed at page 347 of the Schneier book.

Second, Applicant notes that first and second linear orthomorphisms (also known in mathematics literature as complete mappings) are combined to produce the maximal nonlinear block substitution tables (i.e., mappings) recited in claim 1. The first linear orthomorphism is an orthomorphic permutation of the first set of complete linearly independent numbers and the second linear orthomorphism is a different orthomorphic permutation of the second set of complete linearly independent numbers. Combining the linear orthomorphisms is pairing them, not adding or X-ORing them. The first member of the pair is the clear text input and the second member of the pair is the cipher text output. When the generating functions used to produce the first and second linear orthomorphisms are compatible (i.e., the first generating function is compatible with the second generating function), combining the first and second linear orthomorphisms creates block

substitution tables having maximal nonlinearity. In contrast, if the first and second generating functions are not compatible, combining the resulting first and second orthomorphisms will not create block substitution tables having maximal nonlinearity.

Applicant also notes that the maximal nonlinear block substitution tables created by combining the first and second linear orthmorphisms are not orthomorphisms and do not have perfect balance (sometimes referred to as a lack of mutual information).

Third, Applicant submits that the Mittenthal paper is **silent** as to creating maximal nonlinear block substitution tables as recited in claim 1. Rather, Applicant submits that the Mittenthal paper merely describes generating functions which generate orthomorphisms, and shows the orthomorphisms to uniquely possess the information theory property of perfect balance, a property shared by all orthomorphisms, linear or nonlinear.

Thus, Applicant submits that the references of record did not make the invention recited in claim 1 available to the public in the United States prior to the filing date of this application. Therefore, Applicant submits that claim 1, and claims 2-15 which depend therefrom, are not anticipated by the Mittenthal paper. Accordingly, Applicant respectfully requests that the § 102(a) rejections associated with claims 1-15 be withdrawn.

Claims 16-17

Applicant respectfully submits that independent claim 16 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 16. *See* MPEP § 2131 *id.* More specifically, and for reasons similar to those set forth hereinabove with respect to claim 1,

Applicant submits that the paper fails to disclose, among other things, "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" as recited in independent claim 16.

Therefore, Applicant submits that claim 16, and claim 17 which depends therefrom, are not anticipated by the Mittenthal paper. Accordingly, Applicant respectfully requests that the § 102(a) rejections associated with claims 16-17 be withdrawn.

Claims 18-19

Applicant respectfully submits that independent claim 18 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 18. *See* MPEP § 2131 *id.* More specifically, and for reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that the paper fails to disclose, among other things, "setting the maximal nonlinear substitution tables by combining the linear orthomorphisms" as recited in independent claim 18.

Therefore, Applicant submits that claim 18, and claim 19 which depends therefrom, are not anticipated by the Mittenthal paper. Accordingly, Applicant respectfully requests that the § 102(a) rejections associated with claims 18-19 be withdrawn.

Claim20

Applicant respectfully submits that independent claim 20 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 20. *See* MPEP § 2131 *id.*

More specifically, and for reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that the paper fails to disclose, among other things, "creating maximal nonlinear substitution tables by combining the linear orthomorphisms" as recited in independent claim 20.

Accordingly, Applicant respectfully requests that the § 102(a) rejection associated with claim 20 be withdrawn.

Claim 21

Applicant respectfully submits that independent claim 21 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 21. *See* MPEP § 2131 *id.* More specifically, and for reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that the paper fails to disclose, among other things, "creating maximal nonlinear substitution tables by combining the linear orthomorphisms" as recited in independent claim 21.

Accordingly, Applicant respectfully requests that the § 102(a) rejection associated with claim 21 be withdrawn.

Claim 22

Applicant respectfully submits that independent claim 22 is not anticipated by the Mittenthal paper because the paper fails to disclose each and every element of claim 22. *See* MPEP § 2131 *id.* More specifically, and for reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that the paper fails to disclose, among other things, "means for creating maximal

nonlinear substitution tables by combining the linear orthomorphisms" as recited in independent claim 22.

Accordingly, Applicant respectfully requests that the § 102(a) rejection associated with claim 22 be withdrawn.

§ 102(e) Rejections

Claims 16 and 18

Applicant respectfully submits that claim 16 is not anticipated by Luyster because Luyster fails to disclose each and every element of claim 16. *See* MPEP § 2131 *id.* More specifically, Applicant submits that Luyster fails to disclose, among other things, "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" as recited in claim 16.

First, Applicant submits that Luyster is **silent** as to maximal nonlinear substitution tables. Rather, Applicant submits that the encryption methods disclosed by Luyster are primarily based upon bit-moving, bit-shifting, and bit-rotation in successive rounds - **not** on the method recited in claim 16.

Second, Luyster is cited in the Office Action as disclosing "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" at Figure 1, block 44 thereof. Applicant respectfully disagrees with this determination and submits that Luyster, at Figure 1, block 44 thereof, merely discloses a process flow of an RC-5 encryption in which ciphertext consisting of n bits is generated by combining the ciphertext values of segments R0 (Figure 1, block 40) and R1 (Figure 1, block 42) - **not** "setting the maximal nonlinear substitution tables based on a

combination of the linear orthomorphisms" as recited in claim 16.

Luyster is also cited in the Office Action as disclosing "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" at Figure 3, block 88 thereof. Applicant respectfully disagrees with this determination and submits that Luyster, at Figure 3, block 88 thereof, merely discloses a process flow of an encryption method in which ciphertext consisting of n bits is generated by combining the ciphertext values of segments R0 (Figure 3, block 84) and R1 (Figure 3, block 86) - **not** "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" as recited in claim 16. For similar reasons, Applicant also submits that Figure 6 (block 148), Figure 7 (block 188), Figure 9 (block 230) and Figure 14 (block 346) of Luyster also fail to disclose "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" as recited in claim 16.

Luyster is also cited in the Office Action as teaching or suggesting "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" at column 21, lines 25-60 thereof. Applicant respectfully disagrees with this determination and submits that Luyster, at column 21, lines 25-60 thereof, merely discloses using linear combination operators (e.g., addition, subtraction, xor, etc.) to combine blocks or segments of binary numbers - **not** to pair linear orthomorphisms to set the maximal nonlinear substitution tables as recited in claim 16.

Luyster is also cited in the Office Action as teaching or suggesting "setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms" at column 43, lines 16-22 thereof. Applicant respectfully disagrees with this determination and submits that Luyster, at column 43, lines 16-22 thereof, merely discloses adding the left segment R0 with the last

subkey value Klast to produce the ciphertext value for segment R0 - **not** pairing linear orthomorphisms to set the maximal nonlinear substitution tables recited in claim 16. For similar reasons, Applicant also submits that column 45, lines 8-16 of Luyster also fails to disclose pairing linear orthomorphisms to set the maximal nonlinear substitution tables recited in claim 16.

Accordingly, for the reasons set forth hereinabove, Applicant submits that claim 16 is not anticipated by Luyster and respectfully requests that the § 102(e) rejection associated with claim 16 be withdrawn.

Claim 18

For reasons similar to those set forth hereinabove with respect to claim 16, Applicant submits that claim 18 is not anticipated by Luyster and respectfully requests that the § 102(e) rejection associated with claim 18 be withdrawn.

§ 103(a) Rejections

Claims 1-15

Applicant submits that claim 1 is nonobvious over Luyster because Luyster fails to teach or suggest each and every element of claim 1. *See* MPEP § 2143 (stating that one of the elements of a *prima facie* case of obviousness under § 103(a) is that the prior art references, either alone or in combination, must teach or suggest every limitation of the claimed invention). More particularly, Applicant submits that Luyster fails to teach or suggest, among other things, "creating maximal nonlinear block substitution tables by combining the linear orthomorphisms" as recited in claim 1.

As explained previously hereinabove, Applicant submits that Luyster is **silent** as to maximal nonlinear substitution tables and thus fails to teach or suggest this feature.

In addition, Applicant respectfully disagrees with the Examiner's statement that "it would have been obvious to one of ordinary skill in the art at the time of the invention was made to split up the generating function of Luyster into two separate generating functions. Applicant notes that splitting an orthomorphic generating function will not produce two separate orthomorphic generating functions, let alone two orthomorphic generating functions that can be used to generate the first and second linear orthomorphisms used to create the maximal nonlinear block substitution tables recited in claim 1.

Therefore, Applicant submits that independent claim 1 is nonobvious over Luyster. *See* MPEP § 2143 *id.* Applicant further submits that claims 2-15, which depend from claim 1, are also nonobvious over Luyster. *See* MPEP § 2143.03 (stating that if an independent claim is nonobvious under §103(a), then any claim depending therefrom is nonobvious). Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 1-15 be withdrawn.

Claim 17

Claim 17 depends from claim 16. For reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that claim 16 is nonobvious over Luyster because Luyster fails to teach or suggest each and every element of claim 16. *See* MPEP § 2143 *id.* Applicant further submits that claim17, which depends from claim 16, is also nonobvious over Luyster. *See* MPEP §

2143.03 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejection associated with claim 17 be withdrawn.

Claim 19

Claim 19 depends from claim 18. For reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that claim 18 is nonobvious over Luyster because Luyster fails to teach or suggest each and every element of claim 18. *See* MPEP § 2143 *id.* Applicant further submits that claim19, which depends from claim 18, is also nonobvious over Luyster. *See* MPEP § 2143.03 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejection associated with claim 19 be withdrawn.

Claims 20, 21 and 22

For reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that independent claims 120, 21 and 22 are nonobvious over Luyster because Luyster fails to teach or suggest each and every element of these claims. *See* MPEP § 2143 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 20, 21 and 22 be withdrawn.

Obviousness-Type Double Patenting Rejections

Claims 1-22

Applicant respectfully disagrees with the Examiner's determination that claims 1-22 are unpatentable over claims 1-34 of U.S. Patent 6,035,042 (the Mittenthal Patent) and submits that claims 1-22 are patentably distinct over claims 1-34 of the Mittenthal patent.

Claims 1-22 of this application recite block substitution tables having **maximal nonlinearity**. Such block substitution tables are useful for applications where the maximum possible level of nonlinearity is required. For example, the block substitution tables are particularly useful for protecting access to major financial accounts and critical operation plans. Thus, security is of primary importance and speed of table generation (on the order of seconds) is of secondary importance. The generated block substitution tables are not orthomorphisms and have maximal possible nonlinearity.

In contrast to claims 1-22 of this application, claims 1-34 of the Mittenthal patent are related to methods of providing high-speed (on the order of microseconds) table generation for block encryption. Such high-speed cryptographic table generation is useful in systems such as pay-per-view television where successive programs must be encrypted differently. Thus, speed is of primary importance and security is of secondary importance. The generated cryptographic tables disclosed in the Mittenthal patent are always orthomorphisms, possess the associated unique property of lack of mutual information (i.e., perfect balance), and have, at best, a **relatively modest level of nonlinearity**.

Because the block substitution tables recited in claims 1-22 of this application are inherently different than the encryption tables recited in claims 1-34 of the Mittenthal patent (maximal nonlinearity vs. relatively modest level of nonlinearity at best), Applicant also notes that the method of generating the block substitution tables recited in claims 1-22 of this application is distinct from the method of generating the encryption tables recited in claims 1-34 of the Mittenthal patent. For example, unlike the encryption tables recited in claims 1-34 of the Mittenthal patent, the maximal nonlinear block substitution tables recited in claims 1-22 of this application are generated by pairing two linear orthomorphisms.

Therefore, for the reasons stated above, Applicant submits that the claims 1-22 of this application are patentably distinct over claims 1-34 of the Mittenthal patent and respectfully request that the obviousness-type double patenting rejections associated with claims 1-22 be withdrawn.

CONCLUSION

Applicants respectfully request a Notice Of Allowance for the pending claims in the present application. If the Examiner is of the opinion that the present application is in condition for disposition other than allowance, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below in order that the Examiner's concerns may be expeditiously addressed.

Respectfully submitted,

Date: February 9, 2004

Robert A Muha

Robert A. Muha
Reg. No. 44,249

KIRKPATRICK & LOCKHART, LLP
Henry W. Oliver Building
535 Smithfield Street
Pittsburgh, Pennsylvania 15222

Telephone: (412) 355-8244
Facsimile: (412) 355-6501
E-mail: rmuha@kl.com